UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/980,390	03/13/2002	Tomoyuki Asano	275748US6PCT	1041

22850 7590 03/09/2006

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/980,390	ASANO ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-2, 4-6, 9-17, 20-25, 27-28, 31-38, and 41-47* is/are rejected.

7)☐ Claim(s) *3,7,8,18,19,26,29,30,39 and 40* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *06/03, 11/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Applicant filed on 03/13/2002.

2. Claims 1-47 are pending.

Claim Objections

3. The acronym "LSI" in claim 9, 20, 31, and 41 needs to be spelled out.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-2, 5-6, 10-13, 16-17, 21-25, 28, 32-35, 38, and 42-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Park, US Patent No. 5761302.

6. As per claims 1-2 and 24-25:

Park discloses "An information recorder for recording information to a recording medium the apparatus comprising: a transport stream processing means for appending an

arrival time stamp (ATS) to each of discrete transport packets included in a transport stream" in (Col 5 lines 33-40); and "a cryptography means for generating a block key for encrypting a block data including more than one transport packet each having the appended arrival time stamp (ATS) from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and encrypting each block data with the block key thus generated; the data encrypted by the cryptography means being recorded to the recording medium" in (Col 5 lines 33-40).

7. As per claims 5, and 16:

Park discloses "The apparatus according to claims 1 and 13, wherein the block seed includes copy control information in addition to the arrival time stamp (ATS) " in (Col 5 lines 33-40, and Col 6 lines 55-61).

8. As per claims 6, 17, 28, and 38:

Park discloses "The apparatus according to claims 1 and 13, wherein the cryptography means encrypts, with the block key in the encryption of the block data, only data included in the block data and excluding data in a leading area including a block seed of the block data" in (Fig 11A-E, Col 6 lines 15-37).

9. As per claims 10, 21, 32, and 42:

Park discloses "The apparatus according to claims 1, 13, and 24, wherein the cryptography means encrypts block data with the block key according to a DES algorithm" in (Fig 11A-E, Col 6 lines 15-37).

10. As per claims 11, 22, 33, and 43:

Park does not discloses "The apparatus according to claims 1, 13, and 24, further comprising an interface means for receiving information to be recorded to a recording medium, and identifying copy control information appended to each of packets included in the transport stream to judge, based on the copy control information, whether or not recording to the recording medium is allowed" in (Col 6 lines 55-67).

11. As per claims 12, 23, 34 and 44:

Park discloses "The apparatus according to claims 1, 13, and 24, further comprising an interface means for receiving information to be recorded to a recording medium, and identifying 2-bit EMI (encryption mode indicator) as copy control information to judge, based on the EMI, whether or not recording to the recording medium is allowed" in (Col 6 lines 55-67).

12. As per claims 13 and 35:

Park discloses "An information player for playing back information from a recording medium, the apparatus comprising: a cryptography means for decrypting encrypted data recorded in the recording medium by generating a block key for decrypting encrypted data of a block data having an arrival time stamp (ATS) appended to each of a plurality of transport packets from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and decrypting each block data with the block key thus generated " in (Col 5 lines 33-40, Col 6 lines 40-50); and a transport stream processing means for controlling data output on the basis of the arrival

time stamp (ATS) appended to each of the plurality of transport packets included in the block data having been decrypted by the cryptography means " in (Col 5 lines 33-40, Col 6 lines 40-50, and Col 7 lines 15-40).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 4, 9, 14-15, 27, 31, 36-37, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Park, in view of Asano Tomoyuki, Japanese Publication Number 11-224456, hereinafter "Tomoyuki".

15. As per claims 4 and 27:

Park does not discloses "the cryptography means generates a disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, and stores them into the recording medium". Nevertheless, Tomoyuki discloses "Information Processor, Information Processing Method, Providing Medium and Recording Medium" invention, which discloses "the cryptography means generates a disc ID (Para 0032) being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to

the recording medium (Master Key Km, the license key), and stores them into the recording medium" in (Para 0037). Therefore, it would have been obvious at the time the invention was made for one having ordinary skill in the art to modify Park's invention to incorporate the cryptographic means in Tomoyuki's invention to provide access restriction to the content.

16. As per claims 9, 15, 31, 37, and 41:

Park does not discloses "The cryptography means generates a device-unique key from any of an LSI key stored in an LSI included in the cryptography means, device key stored in the information recorder, medium key stored in the recording medium and a drive key stored in a drive unit for the recording medium or a combination of these keys, and generates a block key for encrypting the block data from the device-unique key thus generated and block seed". Nevertheless, Tomoyuki discloses "the cryptography means generates a device-unique key from any of an LSI key stored in an LSI includes in the cryptography means (Para 0035, Equation 1), device key stored in the information recorder (Km, Para 0035), medium key stored in the recording medium (Disc Key, Para 0037) and a drive key stored in a drive unit for the recording medium or a combination of these keys, and generates a block key for encrypting the block data from the device-unique key thus generated and block seed (Sector Key, Eksi, and block header)". Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate Tomoyuki's invention with Park to provide access restriction to the content data.

17. As per claims 14 and 36:

Park does not discloses "The apparatus according to claims 13 and 35, wherein the cryptography means generates the block key for decrypting the block data from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS) appended to a leading one of the plurality of transport packets included in the block data". Park discloses only the data bit stream includes the arrival time stamp in the header of each packet and combines numbers of data packet into block and encrypted using the device key each block including the bit streams with ATS in the header in (Col 5 lines 33-40).

Nevertheless, Tomoyuki discloses the cryptography means generates the block key (sector key) from the sector header in (Para 0036).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Park's invention to incorporate Tomoyuki's cryptography means to uniquely generate the block or sector key for each block or sector to strengthening the protection of data being recorded.

18. Claims 45-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sugimura et al, US Patent No. 6519411, hereinafter "Sugimura", in view of Asano Tomoyuki, Japanese Publication Number 11-224456, hereinafter "Tomoyuki".

19. As per claim 45:

Sugimura discloses " A recording medium having recorded therein a block data including more than one packet included in a transport stream and having an arrival time stamp (ATS) appended to each of the packets and *block seed including the arrival time stamp (ATS)* and store the information in a medium" in (Col 8 lines 40-50 and lines 66-67, and Col 10 lines 18-38). However, Sugimura is silent on "the block data including: *an unencrypted data part having a block seed including the arrival time stamp (ATS)* from which there is generated a block key for encrypting the block data; and an encrypted data part having been encrypted with the block key". Nevertheless, Tomoyuki discloses the "Information Processor, Information Processing Method, Providing Medium and Recording Medium" invention, which includes a method of recording data into a storage medium. The method includes steps of generating a time varying random number to encrypt the sector of data (Para 0023, and 0038). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Sugimura's teaching of appending to each of the packets the arrival time stamp info and incorporate the teaching of Tomoyuki to record securely the information into a storage medium by encrypting using the time-varying random number in the header to securely protect the data from fraudulence copying. However, neither Sugimura nor Tomoyuki specifically teach the timestamp in the data

block header, in which the timestamp is used to generate a unique key to encrypt the block data. Nevertheless, Tomoyuki does teach the steps of generating the time-varying random number to uniquely identify the data block or sector and at the same utilizing the time-varying random number as a key to encrypt the sector of data. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Tomoyuki's teaching to utilize the timestamp info instead of the time-varying random number. It is obviously that both timestamp and time-varying random number has a unique characteristic identifying the block data and they both have a time variable information.

20. As per claim 46:

Sugimura discloses " A program serving medium which serves a computer program under which recording of information to a recording medium is done in a computer system, the computer program comprising the steps of: appending an arrival time stamp (ATS) to each of discrete transport packets included in a transport stream" in (Col 8 lines 40-50 and lines 66-67, and Col 10 lines 18-38); However, Sugimura does not teach "generating a block key for encrypting a block data including more than one transport packet each having the appended arrival time stamp (ATS) from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and encrypting each block data with the block key thus generated". Nevertheless, Tomoyuki discloses the "Information Processor, Information Processing Method, Providing Medium and Recording Medium" invention, which includes a method of recording data into a storage medium. The method includes steps of generating a

time varying random number to encrypt the sector of data (Para 0023, and 0038). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Sugimura's teaching of appending to each of the packets the arrival time stamp info and incorporate the teaching of Tomoyuki to record securely the information into a storage medium by encrypting using the time-varying random number in the header to securely protect the data from fraudulence copying. However, neither Sugimura nor Tomoyuki specifically teach the timestamp in the data block header, in which the timestamp is used to generate a unique key to encrypt the block data. Nevertheless, Tomoyuki does teach the steps of generating the time-varying random number to uniquely identify the data block or sector and at the same utilizing the time-varying random number as a key to encrypt the sector of data. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Tomoyuki's teaching to utilize the timestamp info instead of the time-varying random number. It is obviously that both timestamp and time-varying random number has a unique characteristic identifying the block data and they both have a time variable information.

21. As per claim 47:

Sugimura discloses " A program serving medium which serves a computer program under which playback of information from a recording medium is done in a computer system, the computer program comprising the steps of processing a transport stream to control data output on the basis of the arrival time stamp (ATS) appended to each of the plurality of transport packets; However, Sugimura is silent on "the steps of generating a

block key for decrypting encrypted data in a block data having an arrival time stamp (ATS) appended to each of a plurality of transport packets from a block seed which is additional information unique to the block data and including the arrival time stamp (ATS), and decrypting each block data with the block key thus generated; and processing a transport stream to control data output on the basis of the arrival time stamp (ATS) appended to each of the plurality of transport packets included in the block data having been decrypted in the cryptographic step". Nevertheless, Tomoyuki discloses the "Information Processor, Information Processing Method, Providing Medium and Recording Medium" invention, which includes a method of recording data into a storage medium. The method includes steps of generating a time varying random number to encrypt the sector of data (Para 0023, and 0038). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Sugimura's teaching of appending to each of the packets the arrival time stamp info and incorporate the teaching of Tomoyuki to record securely the information into a storage medium by encrypting using the time-varying random number in the header to securely protect the data from fraudulence copying. However, neither Sugimura nor Tomoyuki specifically teach the timestamp in the data block header, in which the timestamp is used to generate a unique key to encrypt the block data. Nevertheless, Tomoyuki does teach the steps of generating the time-varying random number to uniquely identify the data block or sector and at the same utilizing the time-varying random number as a key to encrypt the sector of data. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the

art to modify Tomoyuki's teaching to utilize the timestamp info instead of the time-varying random number. It is obviously that both timestamp and time-varying random number has a unique characteristic identifying the block data and they both have a time variable information.

Allowable Subject Matter

1. Claims 3, 7-8, 18-19, 26, 29-30, and 39-40 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

22. As per claims 3 and 26:

Park discloses "The apparatus according to claims 1 and 24, wherein the cryptography means generates a title-unique key from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, and generates the block key from the title-unique key and block seed.

23. As per claims 7, 18, 29, and 39:

Park discloses "The apparatus according to claims 1, 13, and 24, wherein the cryptography means generates a title-unique key from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, takes

the thus-generated title unique key as a key for an encryption function, places the block seed into the encryption function, and outputs a result of the placement as a block key.

24. As per claims 8, 19, 30, and 40:

Park discloses "The apparatus according to claims 1, 13, and 24, wherein the cryptography means generates a title-unique key from a master key stored in the information recorder, disc ID being a recording medium identifier unique to a recording medium and a title key unique to data to be recorded to the recording medium, places the title-unique key thus generated and block seed into a one-way function, and outputs a result of the placement as a block key.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100